Chapter 1: Those Pesky Network Things You Need to Know

In This Chapter

- **Finding out why you really *do* want a network, at the office and at home**
- **Comparing client/server (domain) and peer-to-peer (workgroup) networking**
- **Gathering the stuff you need to get started**
- **Networking for Neanderthals**

When business people talk to each other, it's called networking. When computers talk to each other, it's called pandemonium.

This chapter tries to distill 30 years of advances in computer pandemonium, er, networking, into a succinct, digestible, understandable synopsis. I think you'll be pleasantly surprised to discover that even the most obnoxiously inscrutable networking jargon — much of which has made its way into Windows Vista — has its roots in simple concepts that everyone can understand.

COPYRIGHTED MATERIAL

Understanding Networks

Not long ago, networks were considered esoteric and intimidating, the province of guys in white lab coats, whose sole purpose in life was to allow you to print on the company's fancy laser printer or share that super-fast Internet connection but keep you from seeing your boss's personnel file or the company's budget. Those same guys (and they were always guys, it seems) often took it upon themselves to tell you what you could and couldn't do with your PC — what software you could use, how you could use it, where you could put your data, and so much more. They hid behind a cloak of mumbo-jumbo, initiates in the priesthood of "systems administration."

That's changed a lot. With Windows Vista, a network is something that your 13-year-old can throw together in ten minutes. Mine did. (Your results may vary!)

The terminology doesn't help. Ask a network geek — or computer store salesperson — about the difference between a LAN and a WAN, and you'll provoke a tirade of inscrutable acronyms so thick that you need a periscope to see out.

In the following sections, I cut through the bafflegab.

What a network can do for you

Do you need a network? The short answer: Yes. If you have two or more computers, with one running Windows Vista and the other running Windows 98 or later, a network is well worth the hassle. You don't need a fancy one. But you do need one. Consider these facts:

- **If you have a network, just about any piece of hardware attached to one computer can be used by the other.** That dual-scan DVD recorder on your desktop, for example, can be used by your portable, the same way as if it were connected directly. A printer or (in some cases) a scanner attached to one computer can be shared by all computers.
- **All your computers can use a single Internet connection.** When all your computers are connected to a hub or a router, you don't need to pay for two Internet accounts or run two connections (over the phone, or via DSL or cable modem) at the same time. If every computer on the network is downloading huge files at the same time, you'll feel the performance hit, of course, but in most normal circumstances, you won't notice any performance change.
- **You can use Vista's features on data from other machines, regardless of whether they're running Vista.** For example, with Vista's Explorer, you can view pictures stored on a networked computer as a slide show, even if the pictures are stored on a computer running Windows 98. You can burn a DVD with Windows Vista's built-in DVD burning support, using data from any computer on your network. Even the Windows Media Player and Media Center can work with sound and video clips from other machines.
- **You have an easy way to make backups.** The easiest, fastest, most reliable way to back up data is to copy it from the hard drive in one machine to the hard drive in another machine on the network.
- **You can share documents, pictures, music — just about anything — between the networked computers, with practically no effort.** Although

very few applications allow you to share individual files simultaneously — Word doesn't let two people on two different machines edit the same document at the same time, for example — sharing data on networked machines is still much simpler. If you get Windows Meeting Space cranked up (see Book IX, Chapter 2), sharing stuff among Vista PCs is like falling off a log.

How a network networks

All you really need to know about networks you learned in kindergarten. Here's the lowdown:

- Good computers talk to each other over a network. If your computer is on a network, it can play with other computers on the same network. If your computer is not on a network, it can only sit in the corner and play by itself.
- You can see all the computers on your network by looking at Mister Rogers' . . . uh, by choosing Start➪Network.
- Every computer in a network has its own name — actually, it's a number called an *IP address* — and all the names (er, numbers) are different. That's how computers keep track of each other.
- You can share stuff on your computer. You have two different ways to share. The way you share depends on how the network — uh, kindergarten class — is organized:
  - If you have a really mean teacher (called a *network administrator*), she decides what can be shared. When other kids want to borrow your stuff, they usually have to ask the teacher. I don't talk about this kind of network very much because the teacher makes most of the decisions. Details are in the next section of this chapter.
  - On the other hand, if the kids are in charge of sharing, each kid can share his stuff in one of two ways. He can put the stuff that he wants to share in a special place that's called Public (that's a Public folder) and tell Vista that he wants to share it (see Book II, Chapter 1), or he can tell the computer to just go ahead and share the stuff (using a shared folder, shared drive, or a shared printer).
- Your network can share with other networks, just like kids in your class can share with kids in other classes. The Internet is the biggest class of all. Yippie!
- Unfortunately, some creeps are in other classes, and they may want to take things from you or share something that can hurt you. You have to protect yourself.

- When you run into trouble, the advice you hear over and over again (especially in the Vista Help and Support Center) is "talk to your teacher," uh, "contact your system administrator." That advice is every bit as useless now as it was when you were five.

When networks work right — which they do about 90 percent of the time in Vista — they really are simple.

Organizing Networks

To understand an abstract computer concept, nothing works better than a solid analogy. I use lots of them in this book: A document is like a sheet of paper; a CPU is like a car engine; a modem is like a high-tech hearing aid with a pronounced stutter set to "max" at a Nine Inch Nails concert. You know what I mean.

That's the problem with configuring networks. No really good analogies exist for all the bits and pieces. Yes, you can say that a server is like a gatekeeper, or a hub is like a collection of tap-dancing monkeys at a hyperactive organ-grinder's convention, but all the analogies fall flat in short order. Why? Because networks are different from what you experience day to day. So without benefit of a good analogy, I shall forge ahead anyway.

Understanding servers and serfs

Two fundamentally different kinds of networks exist. They both use the same basic kind of hardware — cables, boxes, interface cards, and so on. They both talk the same basic kind of language — Ethernet and something called TCP/IP, usually, but a few renegades speak in tongues. They differ primarily on a single, crucial philosophical point.

In one kind of network, a leader, a top-dog PC, controls things. The leader is called (you guessed it) a *server.* I still get shivers down my spine at the Orwellian logic of it all. In this kind of network, the lowly serf PCs are called *clients.* Thus, this type of network gets the moniker *client/server.* Microsoft calls this kind of network a *domain.* If you've ever wondered how in the realm of the English language a "client" could be all that much different from a "server," now you know: In the topsy-turvy world of PC networking terminology, a server is really a master.

Client/server networks abound in large companies, where central control is crucial. Network administrators set up security rules, grant access where needed, allow new users to operate client PCs, and generally ride herd on the entire network. Usually the server(s) hold important corporate files and backup copies of key files on the client computers. Usually the major

networked printers hang off of the server(s). Usually all Internet access goes through the server(s). Usually.

In the other kind of network, all the pigs, er, PCs are created equal. No single PC dominates — perhaps I should say *serves* — all the others. Rather, the PCs maintain an equal footing. This kind of network is called, rather appropriately, *peer-to-peer,* which sounds veddy British to me. Eh, wot? Microsoft calls them *workgroups,* which isn't nearly as classy.

Peer-to-peer networking doesn't get hung up in the kind of security and central administration that client/server networks take for granted. For example, a typical user on a peer-to-peer network can share a disk drive so that anybody on the network can see it. On a client/server network, you'd have to call in the network administrator.

At the risk of oversimplifying, peer-to-peer networking works best in homes and small offices where security isn't a major concern. Client/server networking works best in larger companies with significant security needs — and a budget to match. Network administrators don't come cheap. So much for the overview. I now take a look at the details.

Introducing client/server networks

Client/server networks have one PC, called a server, that's figuratively "on top" of all the others. Figure 1-1 shows a logical diagram of a client/server network. It's important that you not take the diagram too seriously: It only shows the way client PCs are subservient to the server. It doesn't show you how to hook up a network.

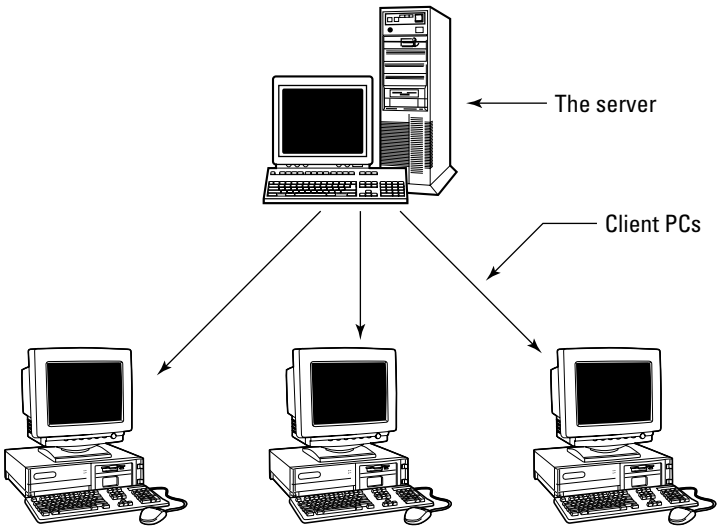

Figure 1-1: Logical view of a client/server network.

Client PCs have some autonomy in a client/server network, but not a whole lot. And a bit of leeway exists in how much security a specific network or server enforces — some less-secure networks may allow guest accounts, for example, that don't require passwords. But by and large, client/server networks are set up to be secure. They exist to allow computers (and users and peripherals) to talk to each other. But strict limits are rigorously enforced on what individual users can do, where they can go, and what they can see.

Microsoft introduced a new umbrella security system in Windows 2000 Server called Active Directory. It's designed to put control of all client/server security activities in one place. Active Directory is a very complex program — a world unto its own. If you have trouble talking to your network administrator in simple English, you may take some solace in the fact that he has to talk to Active Directory, and the translation can be challenging. The African "click" languages pale in comparison.

In general, you want to use Windows Vista Enterprise Edition (or possibly Ultimate) if you're on a client/server network. Yes, you can set up Vista Business Edition to work on a client/server network. No, it isn't worth the effort — or added expense.

In this book, I don't talk about client/server networks (er, *domains*) very much, simply because you don't have much control over them. If you use a client/server network, chances are good that somebody else in your company made the decision to go with client/server. He or she probably installed your copy of Vista — most likely Vista Enterprise — or bought a new machine rigged to his specifications and configured it to work with your company's network. He also gets to fix things when your network connection goes bump in the night. Poetic justice, sez I.

I have to talk about client/server from time to time, though, for three big reasons:

- **You may have an existing client/server network that you want to convert to a peer-to-peer network.** Many Dummies (I'll raise my hand here) installed Windows NT, Windows 2000, or Windows 2003 client/server networks in their homes or offices, and they're tired of the constant hassles. They need to understand enough about client/server to get rid of it.

- **You may actually need some of the features that client/server offers and not know it.** In that case, you are better off to bite the bullet now and get client/server going, instead of struggling with peer-to-peer as an unintentional stopgap.
- **Client/server is the original form of networking** (at least in the business environment; you can argue about academia some other time). As such, many networking concepts — and much of the obscure terminology — originated in the client/server cauldron.

Administrator accounts on client computers can make major changes to the client PC in question, but the real action is on the server. If you really want to change things around, you need an administrator account on the server. That's the seat of power in the client/server milieu.

In a client/server network, the network's Internet connection is (almost) always controlled through the server, using the following:

- **Windows Proxy Server:** A *proxy server* is a program that allows all the people on a network to share one Internet connection and, at the same time, almost always acts as a *firewall.* A server firewall monitors data as it passes between your network and the Internet, acting as a security barrier.
- **Microsoft Internet Security and Acceleration Server:** This is a souped-up, extra-charge proxy server.
- **Other proxy servers:** Many proxy servers are made by companies other than Microsoft. Ositis Software's WinProxy, for example, is used in many companies to protect their client/server networks. (See `www.winproxy.com`. WinProxy works on peer-to-peer networks, too.)

Introducing peer-to-peer networks

On the other side of the networking fence sits the undisciplined, rag-tag, scruffy lot involved in peer-to-peer computing. In a peer-to-peer environment, all computers are created equal, and security takes a backseat to flexibility. I like peer-to-peer networks (see Figure 1-2). Could you tell?

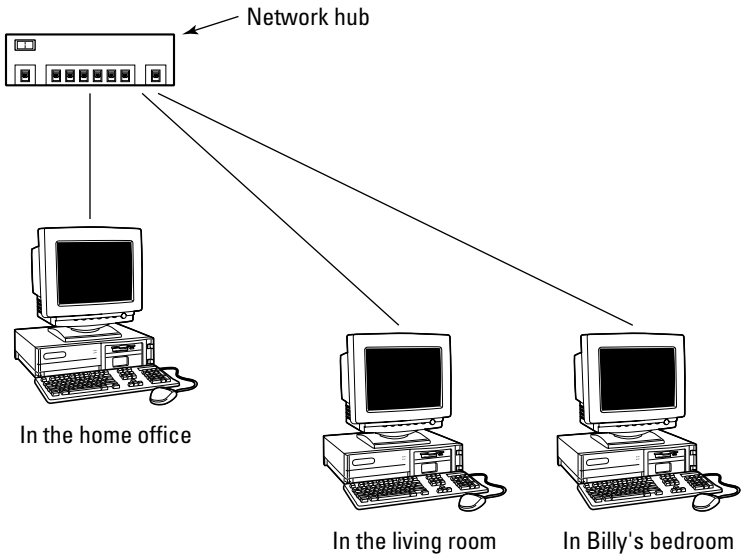

Figure 1-2: Peer-to-peer networks don't rely on a single super PC.

At different times, in different places, Microsoft calls peer-to-peer networks by the following names:

- Workgroups and/or workgroup networks
- Small-office networks and/or small-business networks
- Home networks

The Windows Vista Help and Support Center also, on occasion, refers to peer-to-peer networks as, uh, peer-to-peer networks. They all mean the same thing.

Traditionally, client/server networks (see the preceding section) dangled all the shared peripherals off the server. Fifteen years ago, your office's big laser printer was probably connected directly to the server. The massive bank of 2GB hard drives no doubt lived on the server, too. Even today, you hear reference to *print servers* and *file servers* in hushed tones, as if only the server itself were capable of handling such massive processing demands.

Nowadays, you can buy a laser printer out of petty cash — although you better have a line in the budget for toner and paper — and 500GB hard drives fit on the head of a pin. Well, almost.

Peer-to-peer networks dispense with the formality of centralized control. Every authorized administrator on a particular PC — find out more about administrators in Book II, Chapter 2 — can designate any drive, folder, or piece of hardware on that PC as shared, and thus make it accessible to anyone else on the network.

In a peer-to-peer network (a *workgroup*), any administrator on a given PC can share anything on that PC. If you're the least bit concerned about security, that fact should give you pause, high blood pressure, and intense anxiety attacks. Not to mention apoplexy. Say you set up a home office network using the standard Vista Home Basic settings. The network that is installed is a peer-to-peer network, quite frequently with no passwords. That means anyone can walk up to a Welcome sign-on screen, click one of the usernames, and immediately designate every drive as shared. The entire process would take less than 30 seconds. From that point on, anybody who can get to any of the computers on the network would have full control over all the files on the shared drive — anybody can read, change, and even delete them permanently, without the benefit of the Recycle Bin.

The primary distinguishing factor among PCs in a peer-to-peer network lies in the shared hardware hanging off an individual PC. Refer to Figure 1-2, for

example, and you see that only one PC has a scanner attached to it. Although you may be tempted to call this machine "The PC with the Scanner Hanging off of It," in general parlance, you hear the PC referred to as the scanner's *host.*

Peer-to-peer networks are far more adaptable (computer nerds would say "more robust") than their client/server cousins because they don't rely on a single PC to keep the network running. In a peer-to-peer network, if the laser printer's host PC breaks down, you only need to schlep the printer over to a different PC and install it. You can immediately begin using the printer from any PC in the network. (If auto-detect kicks in properly, it's particularly simple: You only need to change the printer in the File➪Print dialog box.) In a client/server network, if the server PC breaks down, you can probably kiss your weekend good-bye.

To the outside world, your peer-to-peer network appears as if you have just one PC connected to the Internet — and it sits behind a big, scary firewall to fend off would-be attackers. To little Johnny, who's using the PC in his bedroom to download massive full-color pictures of anatomically correct Pokemon figures, his Internet connection works just like it always did: slow and cantankerous, with frequent dropped connections and unexplained outages. But at least everybody in the family gets bumped off the Internet at the same time.

Comparing the p-pros and c-cons

If you need to decide between installing a client/server network (Microsoft calls it a *domain*) and a peer-to-peer network (*workgroup* in MS-speak), you should read the two preceding sections for an overview of how each works, and then weigh each of these factors:

- **The *C* in client/server stands for complicated, cumbersome, and costly.** You, or someone you hire, will spend a lot of time setting up a client/server network. If you have a small network with few employees and one or two applications, you know precisely what machines will be performing which tasks, and you know who needs access to what information and where it's stored, a real pro with extensive Active Directory experience can probably set up your client/server network using Windows Small Business Server in half a day. Beyond that, the sky's the limit — and plan on getting your network consultant's home telephone number, because you're going to need it every time you get a new employee, install a new computer, or maybe even begin using a new application.
- **Client/server networks can handle enormous volumes of data.** High-end servers can juggle hundreds (or even thousands or tens of thousands) of client PCs, with data transmission speeds that would bring tears to a lowly peer-to-peer network's eyes. The server can take on additional functions, such as handling e-mail for the entire network

(most likely using Exchange Server, another cantankerous Microsoft product that's chock full of features). Data backup and other maintenance tasks that would be a nightmare to coordinate over a peer-to-peer network are all localized (that is, wrapped up into a server).

- **The *P* in peer-to-peer stands for powerful, painless, and potentially embarrassing.** If you get your Internet company to install a wireless network, you can have your network up and running in hours — and most of that time will be sweating over sharing printers and Public folders (see Book II, Chapter 1). When it's up, the network will be reliable and easy to use — and as exposed as a lobster in a glass tank. Unless you go to the trouble of setting up and rigorously using passwords (see Book II, Chapter 2), anybody who can sit down at a PC can make all the PC's contents available to anyone on the network, at any time. Except in extreme situations, not even Windows Firewall can help.

If you try to install and maintain a client/server network yourself — even with helper tools such as Microsoft's Small Business Server — be aware that it's not nearly as simple as the marketing brochures would have you believe. Many Dummies, this one included, feel that installing and maintaining your own client/server network rates as a low-benefit, high-commitment time sink of the first degree.

Someday, secure networks will be easy to set up and use. That day hasn't arrived yet. Although peer-to-peer networking in Windows Vista has made simple networking a reality, truly secure networks — and really big networks — are still the province of guys in white lab coats.

Cutting through the Terminology

Peer-to-peer networks work great over wireless connections. If the people who sell you an Internet connection have a wireless box, get it. The installation folks plug the *wireless router* into the phone line or cable TV outlet, and every machine that has a wireless card gets on the Internet with a minimum of fuss.

Confused by the terminology? Don't be. Here's a quick reference:

- A *wireless router* combines the functions of a *wireless access point,* a *DSL or cable "modem,"* and (usually) a *hub.* If you buy or rent a wireless router from your Internet company, you don't have to futz with any of the details — or any of the other terms in this list.
- A *wireless access point* is a box with a pair of rabbit ears on top. PCs with wireless cards talk to the wireless access point.

- A *DSL "modem"* is a box that connects to your phone line and (usually) delivers always-on, fast Internet, most commonly using a technology called asymmetric digital subscriber line (ADSL).
- A *cable "modem"* is a box that does the same thing, but it connects to your cable TV cable.
- A *hub* is a box with a bunch of slots on the back that take local-area network (LAN) cables. The hub connects all the PCs and other boxes that are plugged into it.
- A *LAN cable* looks like an extra-wide phone cable. It's used to connect PCs (usually ones without wireless cards) and other boxes.

If the people who sell you your Internet connection don't have a wireless router, you can use all sorts of combinations to accomplish the same thing. Vista works well with the following:

- **A cable or DSL "modem" attached to the Internet and plugged into a Vista (or Windows XP) PC:** If you only have one PC, that's all you need. If you want to share the Internet connection with more than one PC, you plug a hub into the back of the PC with the Internet connection and plug other computers into the hub. Vista (or Windows XP) can run a program called *Internet Connection Sharing,* which shares the single Internet connection among all the attached computers.
- **A cable or DSL "modem" attached to the Internet and plugged into a hub:** You don't get wireless that way, but any computer close enough to the hub can simply be plugged in, and you all share the Internet connection. This is also a good solution if wireless reception isn't too wonderful and you already have LAN cable pulled through your house or office.
- **A cable or DSL "modem" attached to the Internet and connected in some way to other computers:** Alternatives include using the power lines or using an existing telephone line (HPNA — a de facto home networking standard developed by the Home Phoneline Networking Alliance). You'll need specialized hardware for each computer.

Wired and wireless connections aren't mutually exclusive. Almost every wireless network has the capability for attaching wired computers. In fact, most wireless networks you bump into every day have one or more computers running on wires. They all meet together at the router.

Making Computers Talk

Getting computers to talk to each other can be as simple as buying a box and some cables and plugging it all together like you do with telephones — or as painful, expensive, and hair-challenging (as in pulling it out by the roots) as any computer pursuit you've ever encountered.

In the following sections, I step you through the details of setting up a simple, traditional peer-to-peer network with interface cards in each PC, a *hub* (which is an incredibly dumb switch), and a bunch of cable.

After you see the basics, I step you through the same territory, using wireless technology. If you want to set up a wireless network, I suggest you read about setting up a wired network first (in the next chapter). Walk before you run, ya know?

For details on actually assembling a network — choosing hardware components, installing and testing them, and then getting Windows Vista to recognize the network — see Book IX, Chapter 2.

If you're setting up a new network, chances are very good that you're looking at a wireless peer-to-peer ("workgroup") network. That's a great choice. For the advanced course on wireless networks — surely the simplest kind of network to install — see Book IX, Chapter 3.

Understanding Ethernet

The easiest, fastest, cheapest, most reliable, and most secure way to hook up a peer-to-peer network is also the oldest, least flexible, and most boring. If you want sexy, look somewhere else. If you want an old workhorse, hey, do I have a horse for you: It's called *Ethernet* (see Figure 1-3), and it works like a champ.

Ethernet really isn't that complicated. In the early 1970s, Bob Metcalfe came up with an interesting new way to connect Xerox Alto computers. He called the technique *EtherNet.* The name stuck, give or take a capital *N.* So did the technology. By modern standards, Ethernet isn't very sophisticated. Here's how it works:

- All the PCs on a network watch messages going over a wire.
- When PC *A* wants to talk to PC *B, A* shoots a message out on the wire, saying something like, "Hey *B,* this is *A,*" followed by the message.
- PC *B* sees the message on the wire and retrieves it.

It's hard to believe, but with a few minor tweaks — like what happens when two PCs try to send messages at the same time so that they're talking over the top of each other — that's really all there is to Ethernet.

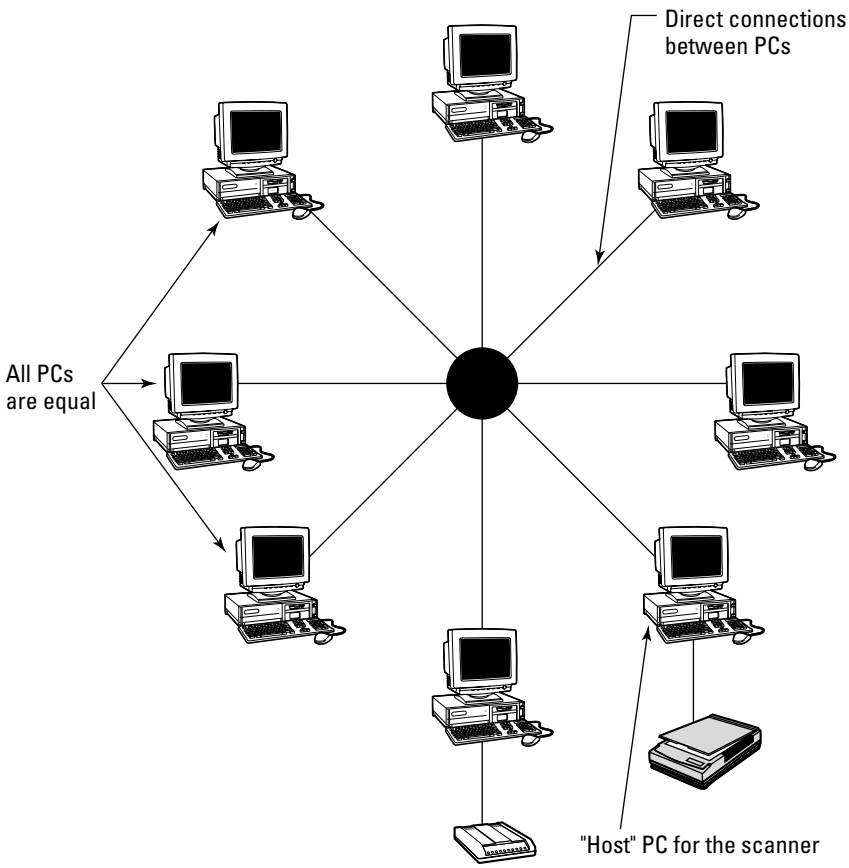

Figure 1-3: A typical Ethernet peer-to-peer network.

Here's what's even harder to believe: PCs using plain old Ethernet can send and receive messages at the rate of 10 Gbps, or 10,000,000,000 bits per second. Even garden-variety Ethernet systems work at 100 Mbps, or 100,000,000 bits per second. (By comparison, a 56K modem, under the best possible circumstances, receives data at slightly more than 50,000 bits per second.) Things get slow if many PCs are trying to talk to each other at the same time — they start talking over the top of each other — but for a typical peer-to-peer network, 100 Mbps (also called 100Base-T) works great.

Ethernet relies on a *hub* — a box — and cables running from the hub to each PC. The PCs need network cards so that you have a place to stick the cables. The PCs can be using any flavor of Windows since Windows 98. Plug it all

together, run the Set Up a Network Wizard on your Windows Vista machine(s), run a special program that Vista sticks on a key disk on the other machines, and your network is ready to use.

That's the theory, anyway. Surprisingly, at least 90 percent of the time, it works. I go into all the details in the next chapter.

Adding wireless

What's the biggest problem with Ethernet? The cables. Unless your office or home has been wired with those big eight-wire Ethernet cables, you have to string them across the floor or under the rug, run them up and down staircases, or hang them out the window and pray they don't blow away. Don't laugh. I've done all that and more.

Wireless networking relies on radio transmitters and receivers in place of Ethernet's cables. You need a wireless access point (which goes by a lot of different names, most commonly WAP, as in, uh, *Whap!*), wireless receivers plugged into each PC (possibly by a card or connected via a USB adapter), or wireless built into the computer (common with laptops).

Wireless networks use the same kind of technology as everyday wireless telephones: The part that moves (the telephone handset) communicates with a base that stays put (the phone cradle). Wireless connections suffer all the problems that you've no doubt encountered with portable telephones:

- The signal gets weaker as you move farther away from the base station, and at some point it disappears.
- If the base gets unplugged, everything goes bananas.
- Other people can eavesdrop on your conversations, unless you're cautious. Ain't no such thing as a free lunch.

I go into detail about wireless networking in Book IX, Chapter 3.